UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

GOOGLE LLC, *Plaintiff,* v. DOES 1–25, *Defendants.*	Civil Action No.: **FILED UNDER SEAL**

COMPLAINT FOR DAMAGES AND INJUNCTIVE RELIEF

Plaintiff Google LLC ("Google"), by and through its attorneys, brings this Complaint against the Defendants for injunctive relief and damages. Google alleges as follows:

INTRODUCTION

1. Defendants are cybercriminals based in China who have silently infiltrated over ten million connected devices—including personal TV streaming boxes, tablets, and projectors—to form a "botnet" (or network) that is leveraged to conduct and conceal a wide range of criminal activity. This botnet—called the "BadBox 2.0" botnet—is already the largest known botnet of internet-connected TV devices, and it grows each day. It has harmed millions of victims in the United States and around the world and threatens many more. Without warning, it could be used to commit more dangerous cybercrimes, such as ransomware[1] or distributed denial-of-service ("DDoS") attacks.[2]

2. Defendants work together to grow, control, and profit from the BadBox 2.0 botnet as part of a criminal enterprise (the "BadBox 2.0 Enterprise" or the "Enterprise") that has surreptitiously preinstalled malware in certain devices and tricked users into downloading free applications ("apps") that contain malware, giving Defendants and other threat actors access to the users' personal devices without the user ever knowing it. Together, these infected devices create a network—the "botnet"—of hijacked consumer devices that Defendants use to commit a range of cybercrimes.

[1] Ransomware is a type of malicious software ("malware") that is designed to block access to all or part of a computer system until a sum of money is paid.

[2] A DDoS attack occurs when multiple internet-connected devices are directed to collectively overwhelm the bandwidth of a particular website or system for the purpose of taking that website or system offline.

3. Once Defendants have infected devices with BadBox 2.0 malware, they use their illicit access to the devices to infiltrate the digital advertising ecosystem by setting up a variety of ways to obtain a fraudulent payout (together, the "BadBox 2.0 Scheme"), including:

a. **Sale of proxy connections**: Defendants sell unauthorized access to victims' infected devices for use as "residential proxies," which, unbeknownst to the victims, are exploited by cybercriminals to conceal their location and internet protocol ("IP") address while committing other cybercrimes, including account takeovers, fake account creation, credential theft, and sensitive information exfiltration.

b. **Advertising fraud**: Defendants are also conducting a variety of ad fraud schemes, including by using the infected device to create fake (i.e., non-human) views of ads that are published to apps downloaded onto the infected device and operate in the background, by directing the infected device to launch hidden web browsers that navigate to a collection of ad-heavy webgaming sites, unbeknownst to the victim owner, or by exploiting pay-per-click compensation models to funnel money to the publisher of a website for fake clicks on real ads.

4. The BadBox 2.0 is Defendants' *second* global botnet. Defendants developed and used a prior iteration of the BadBox botnet to infiltrate devices globally, including in the United States. German law enforcement conducted a disruption operation against the initial iteration of the BadBox botnet in 2023. The BadBox 2.0 botnet is far more innovative, expansive, and dangerous than its predecessor.

5. The BadBox 2.0 botnet, and the criminal schemes it supports, are responsible for causing significant harm to Google, the owners of the infected devices, and countless other entities and individuals.

6. It also causes financial harm to Google, interferes with Google's relationships with its users (and potential users), harms Google's reputation, impairs the value of Google's products and services, and forces Google to devote substantial resources to investigate and combat the botnet's harmful activity.

7. Because of the size and scope of the BadBox 2.0 Scheme, cybersecurity experts have alerted the public, and Google is seeking an injunction to disrupt its infrastructure and stop its spread. Google brings this action under the Computer Fraud and Abuse Act ("CFAA") and Racketeer Influenced and Corrupt Organizations Act ("RICO") against Defendants' criminal enterprise to disrupt the BadBox 2.0 Scheme, to prevent it from causing further harm, and to recover damages.

PARTIES

Plaintiff

8. Plaintiff Google LLC ("Google") is a Delaware limited liability company with its principal place of business at 1600 Amphitheatre Parkway in Mountain View, California.

9. Google operates numerous products, platforms, and services, several of which are relevant here:

a. **Android**: Android is an operating system created by Google that is designed to run on mobile devices, such as smartphones or tablets. Google has both a proprietary version that is used for official Google devices and also released a free version as open-source software. In this Complaint, where we refer to "Android," we refer to Google's proprietary version.

b. **Android Open Source Project ("AOSP")**: AOSP is an open-source software project initially released by Google that is used as an operating system for many devices worldwide. It allows developers to create custom versions of Android. Although AOSP software, like all open-source software, allows anyone to contribute code and software fixes, Google oversees development of AOSP and maintains and further develops Android.

c. **Chrome**: Chrome is a web browser created and operated by Google that runs on various operating systems, including on personal computers, smartphones, and tablets.

d. **Google Ads**: Google Ads is an online advertising platform through which advertisers can publish advertisements on various Google platforms including, for example, Google Search and YouTube.

e. **Google Ad Manager**: Google Ad Manager is a comprehensive ad management platform that allows publishers to sell ad space.

f. **Google Display & Video 360**: Google Display & Video 360 enables marketers to manage their reservation and programmatic-guaranteed campaigns across display, video, TV, audio, and other channels, all in one place.

g. **Google Play**: Google Play is the official app store for certified devices running on the Android operating system, allowing users to browse and download apps developed with the Android software development kit and published through Google. Google Play also serves as a digital content store that offers millions of apps, games, books, and other products to more than 2.5 billion monthly users across over 190 markets worldwide.

h. **Google Play Protect**: Google Play Protect is built-in, proactive protection against malware and unwanted software. It is built into every Android device with Google Play Services. Google Play Protect will automatically warn users and block apps (including apps from stores other than Play) known to contain malware, including malware associated with BadBox 2.0. Android devices undergo extensive testing to ensure quality and user safety. Google maintains records of security and compatibility tests for Google Play Protect devices.

i. **Google Search**: Google Search is an internet-based search engine that allows users to search for publicly accessible documents and websites indexed by Google's servers.

j. **YouTube**: YouTube is an online video sharing platform.

Defendants

10. Defendants Does 1–25 are individuals or entities who have conspired to engage in a pattern of racketeering activity. They have each participated in the operation or management of the BadBox 2.0 Scheme and have engaged in criminal acts that have caused harm to Google, its users, and countless others. Upon information and belief, Defendants are based in China.

11. At this time, Google does not know the true names and capacities of the Doe Defendants sued as Does 1–25 and therefore sues these Defendants by fictitious names. Each of the Doe Defendants is responsible in some manner for the conduct alleged, having agreed to become part of the BadBox 2.0 Enterprise.

12. Google is presently aware of several connected Doe threat actor groups that operate the BadBox 2.0 botnet and support various aspects of the criminal schemes it enables through the BadBox 2.0 Enterprise. It is not clear how many threat actors compose each group nor how many

groups built, control, or use BadBox 2.0; the Doe numbers are meant to be representative. All of the threat actor groups are connected to one another through overlapping infrastructure and historical and current business ties. Each group's misconduct is described in more detail below.

JURISDICTION AND VENUE

13. This Court has federal-question subject matter jurisdiction over Google's CFAA and RICO claims, pursuant to 18 U.S.C. §§ 1030 and 1961, respectively.

14. Defendants are subject to personal jurisdiction in this district, and the exercise of jurisdiction over Defendants is proper pursuant to 18 U.S.C. § 1965 and N.Y. C.P.L.R. §§ 301 and 302. Defendants have transacted business and engaged in tortious conduct in the United States and in New York that gives rise to Google's claims. Defendants also have engaged in intentional, wrongful, illegal, and/or tortious acts, the effects of which Defendants intended to and knew would be felt in the United States and New York. Among other things, Defendants have intentionally caused BadBox 2.0 malware to be downloaded on victims' devices in this district, in New York, and throughout the United States; have intentionally directed victims' devices in this district, in New York, and throughout the United States to participate in intentional, wrongful, illegal, and/or tortious acts; and have directed multiple forms of communication to devices in New York and throughout the United States for the purpose of planning and carrying out their conspiracy and fraud. Defendants were aware of the effects in the United States and New York of those acts; the activities of their co-conspirators and agents were to the benefit of Defendants; and their co-conspirators and agents were working at the direction, under the control, at the request, and/or on behalf of Defendants in committing those acts.

15. Defendants have affirmatively directed actions at the United States, including the Southern District of New York, by attempting to and successfully infecting more than 170,000 devices in New York, including 65,000 devices in the Southern District of New York alone; selling

residential proxy services of consumers in the Southern District of New York; engaging in ad fraud in the Southern District of New York; and engaging in click fraud in the Southern District of New York. Defendants have aimed each of these illegal activities at individuals within the Southern District of New York.

16. Defendants have also intentionally targeted and harmed Google, a company based in the United States.

17. Venue is proper in this judicial district under 28 U.S.C. § 1391(c) because Defendants are not residents of the United States and may therefore be sued in any judicial district. Venue is also proper in this judicial district under 28 U.S.C. § 1391(b) and 18 U.S.C. § 1965 because a substantial part of the events or omissions giving rise to Google's claims occurred in this judicial district, because a substantial part of the property that is the subject of Google's claims is situated in this judicial district, because a substantial part of the harm caused by Defendants has occurred in this judicial district, and because Defendants transact their affairs in this judicial district. Defendants engage in conduct availing themselves of the privilege of conducting business in New York and utilize instrumentalities located in this judicial district to carry out acts alleged herein.

FACTUAL ALLEGATIONS

Google's Relevant Products and Services

18. Google is a leading technology company that offers a wide variety of products and services to governments, businesses, and consumers. Many of Google's consumer-facing products and services are available at no or low cost. Google's mission is to organize the world's information and make it universally accessible and useful. Google has many different revenue streams, including revenue generated from delivering relevant, cost-effective online advertising; cloud-based solutions that provide enterprise customers with infrastructure and platform services

as well as communication and collaboration tools; and sales of other products and services, such as fees received for subscription-based products, apps and in-app purchases, and devices.

19. To facilitate the use of its search service on a wide range of devices, Google developed Android, a mobile operating system designed for touchscreen devices like smartphones and tablets. Android is the world's most widely used operating system.

20. Many Android devices come equipped with Google Play, the app store for the Android operating system, which allows users to browse and download apps, games, movies, books, and other digital content. Through Google Play, Google offers an app-distribution platform where developers can upload their creations and users can download the content they want. All Google Play apps go through a rigorous security analysis before they are published on Google Play, ensuring the apps on Google Play will not harm users' devices. Android devices equipped with Google Play also have Google Play Protect built into the device. Google Play Protect warns users about malicious apps that are downloaded from other sources too. It watches out for any app that might harm your device, keeping Android users safe.

21. In 2008, Google released an open-source Android operating system for free, creating the AOSP. AOSP is an open-source project to manage the software that is used as the operating system for many devices worldwide. The AOSP software is primarily licensed under the Apache License, which allows users to reuse and modify the code for free. Though many devices run on the proprietary Android version developed and still owned by Google, manufacturers other than Google can use AOSP software as an operating system for their devices. Google and the open-source software community dedicate developer time to continually updating and improving AOSP. Although Google retains a significant role in overseeing and approving the development

of AOSP, because it is an open-source resource, anyone can suggest modifications to AOSP software by contributing code (e.g., bug fixes, new features, security improvements).

22. A wide range of internet-connected devices run on variations of AOSP software; however, devices that run on AOSP software or a modified version of AOSP software do not come equipped with Google Play Protect.

23. Google generates revenue from its advertising products, all geared toward delivering relevant ads and providing consumers with useful commercial information.

24. By helping publishers monetize their content and advertisers reach prospective customers, Google helps to enable a free and open internet. Google's broad suite of advertising and analytics tools helps millions of companies grow their businesses every day. These products facilitate online advertising and collectively make up the Google Ad Network.

25. Google constantly invests in and improves its advertising programs. Today, Google Ads is a world-class ad technology platform for advertisers, agencies, and publishers to power their digital marketing or monetization. A core focus of the product is serving relevant ads at the right time in a non-intrusive manner and ensuring advertisers have effective tools to target and to measure the effectiveness of their ad campaigns.

26. Google strives to provide its users worldwide with safe and secure platforms. Google has therefore invested substantial resources to identify, understand, and ultimately disrupt harmful malware.

27. Google has allocated, and continues to allocate, substantial resources to restricting fraudulent ads and protecting users on the web. These include, among other things, filtering out invalid traffic, removing bad actors and billions of improper ads from Google systems every year,

and closely monitoring the sites, apps, and videos where ads appear to ensure that advertisers and the free internet are protected.

28. As part of its ongoing commitment to cybersecurity, Google partners with cybersecurity firms and has dedicated resources to identify and thwart attacks that result from the operation of botnets.

29. For example, in 2023, Google partnered with cybersecurity firms and German Law enforcement to investigate a botnet known as BadBox. As part of that investigation, Google discovered over 74,000 Android devices infected with malware that created "backdoors" on the devices that connected to a command-and-control server when powered on for the first time. German law enforcement conducted a disruption operation against the BadBox scheme.

BadBox 2.0

30. While monitoring the remaining BadBox infrastructure for adaptation, Google and its cybersecurity partners discovered new servers that hosted a list of malicious software targeting AOSP devices. That led Google and its partners to discover a new and complex botnet known as "BadBox 2.0." The BadBox 2.0 operation is a major expansion and adaptation of the BadBox operation. It involves many of the same criminal actors whose *modus operandi* is to develop schemes that target every stage of the customer journey.

31. Like its predecessor, BadBox 2.0 is a large "botnet" through which Defendants conduct their criminal and fraudulent activities.

32. A botnet is a network of internet-connected "bots," each of which is infected by "malware."

33. A bot (short for "robot") is a computer or device that is infected by malware that allows it to be directed to conduct specific activities.

34. Malware is "malicious software" that is generally designed to damage, destroy, disrupt, or steal data from the device on which it is installed. A device user typically installs malware unintentionally, often when asked, for example, to click on a link, open an attachment to an email, or install app software that, unknown to the user, triggers the download and installation of the malware on the user's device. In colloquial terms, the device is then infected with a computer virus. Malware can also be preinstalled on a device if a cybercriminal has access to a device prior to the user receiving it. A user is not typically aware that a device has been commandeered into a botnet. An infected device may appear to act normally to the user despite being controlled by the botnet behind the scenes.

35. Any internet-connected device that is infected with malware can become a bot. That includes laptop and desktop computers, smartphones, tablets, digital projectors, and even other consumer devices within our homes, such as internet-connected streaming boxes that are a part of or connected to televisions (making them "Connected TVs," "CTVs," or "Smart TVs"). Even "smart" refrigerators or thermostats can be commandeered to become bots.

36. A botnet is directed by "command-and-control" servers ("C2 Server"), which can instruct the devices composing the botnet to perform any number of disruptive or even criminal tasks. A C2 Server is typically controlled remotely by individual operators, referred to as "bot controllers," "bot operators," or "bot masters."

37. The botnet's computing power grows with each new device that is infected. Thus, depending on the volume of devices comprising the botnet, the bot controllers can marshal an astonishing amount of computing power to commit cybercrimes. For example, botnets can be used to orchestrate DDoS attacks, in which numerous computers (without the owners' knowledge)

simultaneously send requests to a single website or resource. The attacker can overwhelm the target, rendering the website or other internet-based service unusable.

38. Botnets also can be programmed to steal personal information, financial information, usernames, and passwords from infected devices. They can send emails without the owner of the infected device's knowledge or consent. They can "proxy" or "relay" internet communications to mask the location of bad actors, thereby concealing and facilitating criminal conduct. They can send additional malware to infect other computers. And they can act as a vector to spread ransomware or propaganda, including to interfere with elections or influence public policy. In other words, botnets are both powerful and flexible tools to commit cybercrimes.

39. As of April 2025, BadBox 2.0 is comprised of more than ten million infected AOSP-based TV streaming boxes, tablets, projectors, and after-sale car infotainment systems, including versions of the devices pictured below. In fact, BadBox 2.0 is the largest botnet of infected CTVs ever uncovered and expands beyond CTVs to include additional devices such as tablets, digital projectors, and others.

40. Importantly, the infected devices are not Android TV OS devices or Google Play Protect-certified Android devices, which include Google's proprietary protections against malware attacks. They are devices manufactured by the BadBox 2.0 Enterprise with a modified AOSP-based operating system that do not have the latest AOSP security updates, nor do they have Google's protections present on Android devices and are therefore more vulnerable to attack.

The Enterprise's Roles in the BadBox 2.0 Scheme

41. The BadBox 2.0 Enterprise includes several connected threat actor groups that design and implement complex criminal schemes targeting internet-connected devices both before and after the consumer receives the device. While each member of the Enterprise plays a distinct role, they all collaborate to execute the BadBox 2.0 Scheme. All of the threat actor groups are connected to one another through the BadBox 2.0 shared C2 infrastructure and historical and current business ties, as described below.

42. First, the Enterprise includes groups that develop the BadBox 2.0 infrastructure. They set up C2 Servers and backdoor capabilities to create and control the botnet and have full access to and control of the infected devices. These groups include:

a. **The Infrastructure Group**: This group established and manages BadBox 2.0's primary C2 infrastructure (C2 Servers and domains), which facilitates the BadBox 2.0 Scheme. This group also established and managed infrastructure used by the original BadBox botnet.

b. **The Backdoor Malware Group**: This group is a collection of threat actors who develop and preinstall backdoor malware in the bots. Through that malware, they operate a portion of the BadBox 2.0 botnet and sell access to proxy bots (infected

devices). With that access, this group also has carried out a variety of fraud schemes, including ad fraud.

43. Second, the Enterprise includes groups that develop and operate secondary infrastructure, scheme-specific malware, and scheme-specific apps and websites that are deployed to or used on the infected devices. This infrastructure includes domains and C2 Servers used to operate various malware packages (sets of files that contain malicious lines of code) and to monetize ad space. **Appendix A** lists the known domains used by the BadBox 2.0 Enterprise, as well as the registrars[3] for each domain. The groups comprising this segment of the Enterprise operate various malware packages to conduct fraudulent schemes, such as providing downstream proxy access to infected devices or to conduct ad fraud. These threat actors include:

a. **The Evil Twin Group**: This group creates apps responsible for an ad fraud campaign that relies on using "evil twin" apps to generate numerous ads. These apps also launch hidden web browsers that load hidden ads.

b. **The Ad Games Group**: This is a China-based group connected to a hidden web browser scheme conducted through BadBox 2.0-infected devices that uses fraudulent "games" to generate ads.

44. All of the threat actor groups are connected to one another through the BadBox 2.0 shared C2 infrastructure and historical and current business ties, as described below. There is no reason for these groups to share the BadBox 2.0 C2 infrastructure other than to facilitate their joint participation in the BadBox 2.0 Scheme alleged throughout this Complaint.

[3] Registrars handle the reservation of domain names as well as the assignment of IP addresses associated with domain names.

45. The Enterprise works together to carry out the BadBox 2.0 Scheme; none of the schemes can generate revenue without multiple members' participation and coordination. The Enterprise forms a centralized C2 Server ecosystem, develops, exploits, and sells backdoor access to individual devices to connect those devices to the central C2 Servers, and uses that access to attack the digital advertising ecosystem from multiple angles.

Fraudulent Schemes Perpetrated by the BadBox 2.0 Enterprise

46. The BadBox 2.0 Enterprise has worked in concert to construct the BadBox 2.0 botnet and infrastructure and deploy it to commit downstream cybercrimes or to sell access to it so that others may commit cybercrimes.

47. To develop the botnet, the BadBox 2.0 Enterprise first infects AOSP devices by installing malware to create a "backdoor" (i.e., access point) to the device through one of two methods: preinstallation or download by the user.

48. **Preinstalled Malware**. In the BadBox 2.0 Scheme, the Enterprise purchases devices from a handful of Chinese manufacturers and installs a modified version of AOSP on those devices to facilitate the installation of a "backdoor" on the devices. The devices are programmed to connect to the Enterprise's C2 Servers when they are powered on for the first time. The device can then be instructed by the C2 Servers to download additional malware that facilitates ad fraud and other types of crime.

49. **Downloaded Malware**. The backdoor malware can also hide in a downloadable app. The BadBox 2.0 Enterprise tricks users into downloading the backdoor malware onto AOSP devices that are not equipped with Google Play Protect. To do so, the Enterprise creates malicious apps that appear benign (and may even be available in app stores like Google Play in their benign form). Because the malicious app appears identical to the benign app, users are tricked into

downloading the malicious app from an unofficial app marketplace. These malicious apps may, to some extent, function in a similar way to the benign app, which often prevents the user from realizing that the app is malicious. Once the user downloads the infected app, the malware will connect the device to a C2 Server (provided the device is not equipped with Google Play Protect).

50. Regardless of whether the initial infection occurs through preinstallation or through a download by an unsuspecting user, the result is the same: Malware on the device results in a backdoor connection to the Enterprise's C2 Servers that gives the C2 Servers persistent access to the device and the ability to communicate with it. Once the C2 Server has command and control of the device, it can direct the device to download additional malware to support the BadBox 2.0 Enterprise's criminal activity. BadBox 2.0 is particularly dangerous not only due to its scale, but also its flexibility. The Enterprise designed its infrastructure to facilitate a wide variety of criminal schemes and fraudulent operations, including selling proxy connections to infected residential devices and at least three different types of ad fraud.

51. Each illegal scheme generates revenue for the BadBox 2.0 Enterprise.

52. **Sale of Residential Proxy Connections**. The Enterprise uses BadBox 2.0 to sell unauthorized access to individual bots (infected devices) or a botnet (a network of infected devices) that act as "proxies." Cybercriminals pay the Enterprise to use these "proxy" devices as a mask to conceal their web traffic and other activities in order to prevent their criminal activities from being traced back to them.

53. A cybercriminal will pay to connect to a bot and use that bot's IP address. An IP address is a unique digital fingerprint that provides information about the user and his activity.

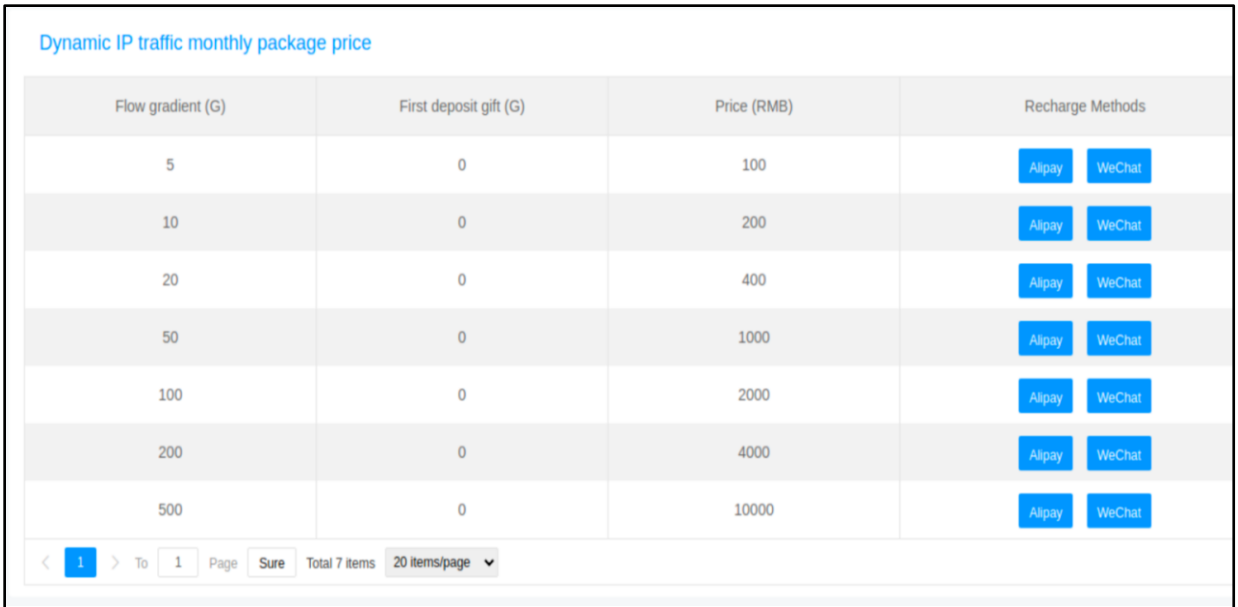
54. Using a "proxy" gives the appearance that the owner of the infected device is engaging in an activity, when instead it is the cybercriminal remotely accessing the device.

55. Victims do not know that their devices have become infected bots, let alone that the devices are being used to mask the illicit activities of others. Nevertheless, their devices may be flagged as malicious as a result of the cybercriminal's activity, preventing the owner from using their device for normal activities.

56. Once the cybercriminal has access to a proxy, he can covertly commit a wide variety of cyber-attacks. He can steal information from the infected computer or other networks, steal passwords, take over accounts, create fake accounts, commit ad fraud, "web-scrape" to obtain user data, conduct a "scalping attack" to buy sought-after products to sell them at a higher price, distribute more malware to commit other types of crime or to connect the bot to other C2 Servers, or conduct a DDoS attack to flood a target server, website, or network with traffic and shut the server down.

57. The BadBox 2.0 Enterprise openly advertises illicit proxy connections obtained through the BadBox 2.0 botnet. As set forth below, the Enterprise charges per gigabyte ("GB") of data routed through the connection per month; on at least one of the Enterprise's websites, they charged $13.90 per 5 GB, and up to $1,390.00[4] for 500 GB.

[4] The dollar amounts are an estimate based on publicly available conversion rates on May 27, 2025. The prices on the website are listed in Chinese Yuan.



Dynamic IP traffic monthly package price

Flow gradient (G)	First deposit gift (G)	Price (RMB)	Recharge Methods
5	0	100	Alipay WeChat
10	0	200	Alipay WeChat
20	0	400	Alipay WeChat
50	0	1000	Alipay WeChat
100	0	2000	Alipay WeChat
200	0	4000	Alipay WeChat
500	0	10000	Alipay WeChat

1 To 1 Page Sure Total 7 items 20 items/page

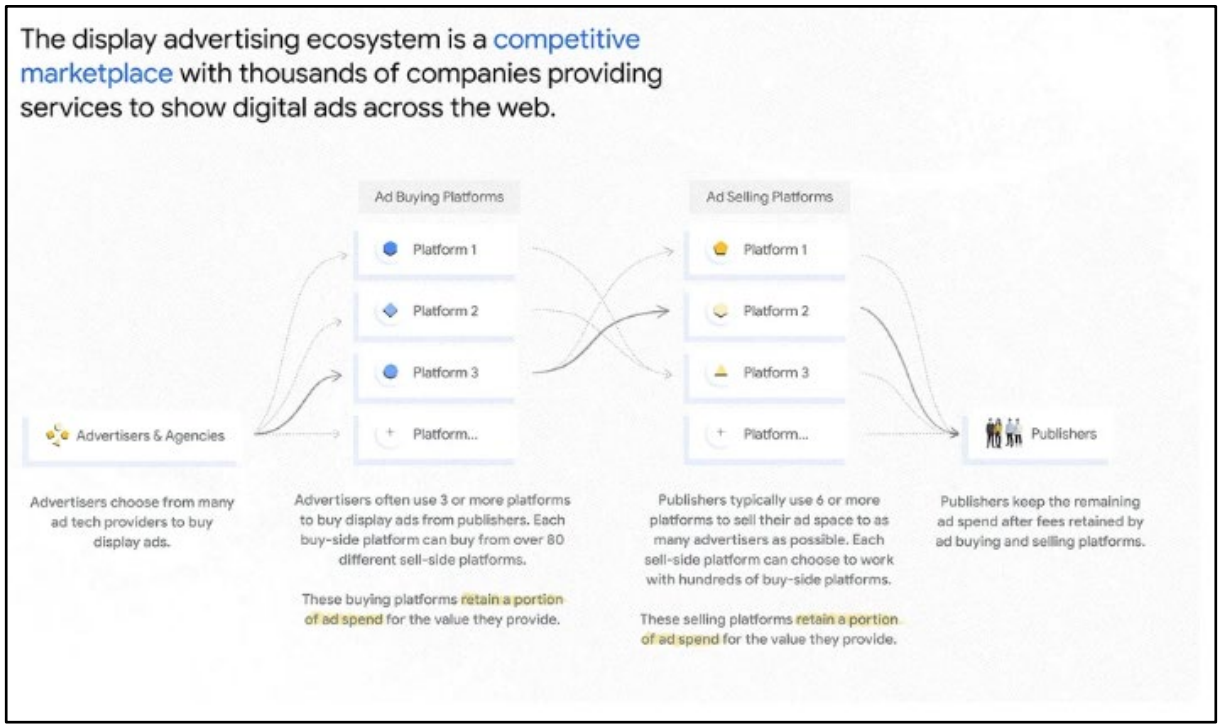
Residential proxy services offered by MoYu, routed through BADBOX 2.0-infected devices (second image is a translation of the first)

58. For example, the Enterprise's residential proxy services have been used to facilitate at least one large scale ad fraud scheme called "Apollo." The Apollo scheme generates fake ad traffic equivalent to the traffic of a mid-sized city like Stamford, Connecticut.[5]

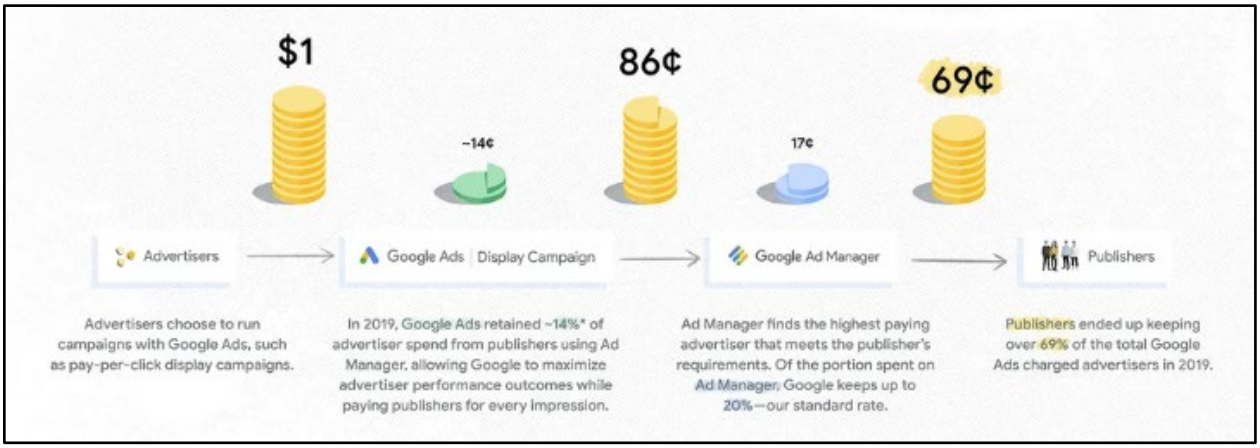
59. **Ad Fraud**. The BadBox 2.0 Enterprise also uses the BadBox 2.0 botnet to commit ad fraud. As a general matter, ad fraud occurs when a scammer intentionally manipulates online advertising programs. They generate fake clicks, views, or downloads and trick advertisers and ad networks into paying them for advertising that ultimately is not viewed by a real person.

60. Internet advertising involves many parties interacting in real time. On one side are publishers of websites that offer ad space for sale. On the other are advertisers seeking to sell their ads. In the center of these two markets are platforms that facilitate this exchange.

[5] Tony Bradley, *Apollo Exposed: What 400M Fake Ad Requests Reveal About Fraud*, Forbes, https://www.forbes.com/sites/tonybradley/2025/04/17/apollo-exposed-what-400m-fake-ad-requests-reveal-about-fraud/ (Apr. 17, 2025).



61. Google Ads and Google Display & Video 360 provide an online platform to facilitate ad transactions. Every day, millions of advertisers use the Google Ad Network to buy "search ads" (ads placed on search engine results pages) and "display ads" (ads that appear on websites, apps, or other digital platforms). Advertisers use the Google Ad Network to run ad campaigns, and publishers use the Google Ad Network to sell ad space on their websites.



62. The sale and delivery of digital advertising on these platforms is automated. When a user navigates to a browser with ad space, a request to fill the ad space is sent to Google Ad

Network's exchange platform. In response to the request, Google Ads determines which advertiser will fill that space and delivers the ad to the publisher to fill in the ad space on its website.

63. For most display ads, Google pays publishers per impression for every 1,000 "impressions" the ad generates. An impression occurs when an ad is delivered, displayed on a site, and viewed by a user.

64. When advertisers use Google Ads to buy display ads, in most cases advertisers pay Google only when a user takes an action after seeing their ad, such as clicking on the ad or making an order. This is because advertisers using Google Ads are paying for real users to interact with their advertisements.

65. Although Google usually only charges these advertisers when a user takes an action (e.g., clicks on an ad), Google pays publishers for their ad space based on the number of impressions (rather than clicks). This accommodates both advertisers' preferences (to pay per action, such as for a click or conversion) and publishers' preferences (to be paid for the ad slot (i.e., impression) independent of whether the user takes any action or not).

66. Some members of the BadBox 2.0 Enterprise create publisher accounts on the Google Ad Network to offer the ad space on their apps or websites. When their apps or websites are accessed, they request ads from the Google Ad Network and once ads are delivered, the Enterprise receives compensation from Google for ads displayed on their apps or websites.

67. The BadBox 2.0 Enterprise publishes apps or websites with ad space that advertisers buy through Google. The sole purpose of the Enterprise's apps and websites is to provide ad space for BadBox 2.0 bots to generate traffic. The Enterprise will deploy BadBox 2.0 bots to "view" those ads, generating numerous impressions of the ad. Google pays the BadBox 2.0 Enterprise, including the Enterprise and other publishers buying their services, for those

impressions. When the traffic is fraudulent, Google refunds advertisers for any payments made due to the fraudulent traffic.

68. The BadBox 2.0 Enterprise deploys BadBox 2.0 bots to commit and profit from ad fraud on the Google Ad Network in at least three ways: (1) they use Enterprise-created apps to embed hidden ads within bots, (2) they direct the bots to open hidden web browsers to view ads on Enterprise-created websites, or (3) they direct the bots to click on ads to generate revenue for the Enterprise.

69. *Hidden Ads*. In this scheme, the BadBox 2.0 Enterprise preinstalls home-screen launcher apps onto infected devices. Although these apps appear to the user to function normally, when opened, they silently contact an Enterprise-operated C2 Server. The C2 Server then either side-loads code on individual bots to request and render ads or instructs the device to download additional apps that request and render ads that are also hidden from the user.

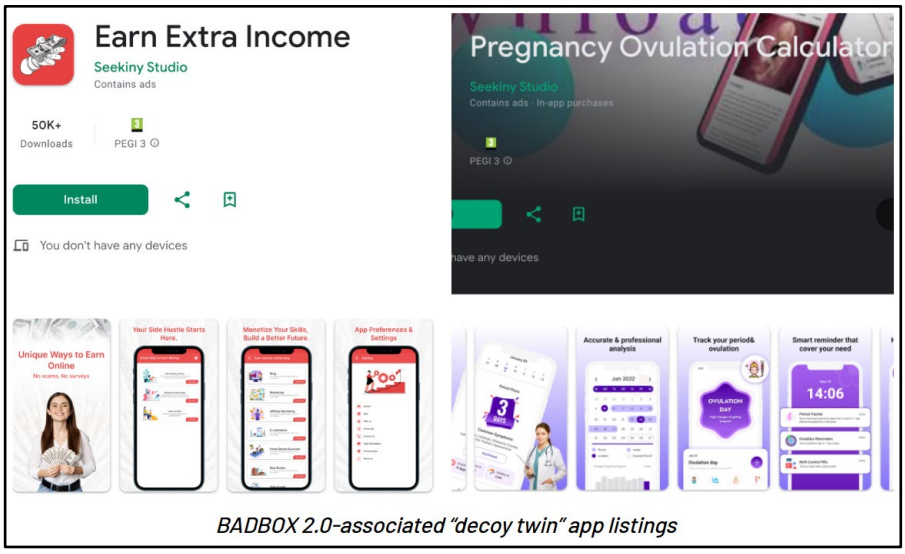
70. To conceal the fraudulent nature of these additional apps, the Enterprise uses a "twin" strategy to disguise the malicious apps.

71. The Enterprise first creates a "decoy twin." These apps—which are available to download on a legitimate app store, such as Google Play—do not contain malware, but serve to legitimize the malicious apps in the event a user or advertiser tries to search for the app. The existence of the decoy twins also legitimizes ad requests from Defendants' malware.

72. The Enterprise then creates a second app—an "evil twin." These apps appear to be nearly identical to the Enterprise-created decoy twins but are in fact malware. Enterprise-operated C2 Servers remotely install these evil twin apps on infected devices. Because the evil twins resemble the decoy twins and, to some extent, function in the same way, device users do not realize

that the apps are malware. If a device user checks a secure app store, the user will see the decoy app and may believe its evil twin is a legitimate app.

73. For example, the decoy twin apps below—"Earn Extra Income" and a "Pregnancy Ovulation Calculator," published by "Seekiny Studios"—were uploaded in order to make the app and its ad requests appear legitimate.



BADBOX 2.0-associated "decoy twin" app listings

74. These "decoy twin" apps hosted in Google Play have thousands of downloads but no reviews. Indeed, even though they are promoted as apps for mobile devices, nearly all the ad traffic that "Earn Extra Income" and "Pregnancy Ovulation Calculator" have generated came from evil twin versions of the apps located on BadBox 2.0-infected devices.

75. The evil twin apps also spoof technical characteristics of the decoy twins. As a result, ad requests coming from evil twins appear as legitimate requests from the decoy twin.

76. To evade security systems designed to detect non-human ad requests, the Enterprise uses its C2 Servers to send commands to the bots to regulate the ad traffic that the evil twin apps create by placing controls on the volume, rate, and types of ads requested.

77. The BadBox 2.0 hidden ads scheme has generated billions of fraudulent requests to render ads in a single week, triggering payouts to Enterprise publishers. One such example is described below.

a. On September 16, 2024, researchers turned on an infected device and connected it to the internet in the United States. The device immediately downloaded a file from a C2 Server named file.long.tv, and the C2 Server began side-loading malicious apps to the infected device.

b. Among the malicious apps the C2 Server instructed the infected device to download was an app named "Pregnancy Ovulation Tracker."

c. The malicious "Pregnancy Ovulation Tracker" app then opened a hidden web browser and began requesting ads from the Google Ad Network, which were rendered in the hidden web browser. The delivery of the ads triggered a payout from Google to the publisher of the app for the impression of the ads.

d. In September 2024, Google identified a version of the app—its decoy twin—on Google Play. Although that version of the app had the same package name and identifier—"com.pregnancy.ovalution.tracker."—it did not appear to have any malicious or suspicious functionality. Nearly all of the ad traffic "Pregnancy Ovulation Calculator" has generated came from BadBox 2.0 devices.

78. *Hidden Web Browser Activity*. The BadBox 2.0 Enterprise also uses its C2 Servers to deploy malware packages that direct infected devices to interact with advertisements and submit fraudulent requests for ads on hidden web browsers that users cannot see in order to generate revenue for the Enterprise.

79. This scheme begins once the Enterprise activates the backdoor to the device. With that access, the Enterprise can direct the bots to open hidden browsers and then navigate to websites created by the Enterprise that feature online games. Each gaming website is filled with ad space. Once the bot reaches a gaming website, it mimics a real user and starts to play the games. Each "game," however, is not designed to engage real players—it prompts an ad to appear every few seconds of play and is designed to trigger as many ad requests as possible. Because the Enterprise publishes the gaming websites, it receives compensation from Google's ad platform for each ad request.

80. One example of this activity is described below.

a. On September 20, 2024, researchers powered on an infected device in the United States and observed it immediately retrieve a malware package named "com.mz.sdk" from an Enterprise C2 Server. The device then downloaded submodules that created a new web browser and sent another request to the C2 Server. The C2 Server responded with instructions that caused the device to take a series of actions designed to evade fraud detection programs by impersonating a real, human user, such as scrolling within the window, accepting cookies, clicking on elements on the page, and visiting search engines.

b. The C2 Server then instructed the device to navigate to a game site called "elitegameu" and to scroll and click on specific pixels on the game site, again mimicking the actions of a real user.

c. Once the device navigated to the gaming site, it selected a game and began to "click" in a manner designed to appear as though a user was playing the game. Every few seconds, however, ads popped up, interrupting the game. By clicking

through the game, the device caused numerous ad requests to be sent to the Google Ad Network.

d. Each time an ad popped up, a request was sent to fill the ad space, an ad was delivered, and Google paid the publisher of the website. Each ad was displayed in the hidden web browser, invisible to the device's user.

81. The BadBox 2.0 Enterprise also uses hidden web browsers to abuse paid search ad programs. The BadBox 2.0 Enterprise adds a search bar to websites they have created that allow ads to show in the search results on their websites. The Enterprise then instructs bots to enter a particular search string on a search engine to silently trigger the delivery of an ad in the search results. The bot will click on the ad link to the website in the search bar, which generates search revenue for clicks on its websites without any real user ever clicking on the sponsored search result.

82. One example of this activity is described below.

a. On September 23, 2024, researchers observed a C2 Server instruct a device in the United States to visit the website app-goal.com—a website controlled by the Enterprise—in a hidden web browser and navigate to Google Search. Once the device navigated to Google Search, the device connected with app-goal.com again and requested a keyword for a search. App-goal.com responded with a keyword for the device to use in a search.

b. This response triggered the device to load a new page in the hidden web browser—a Chrome web browser—that seeded the URL with the keywords, which simulated entering the keyword into the search bar. The device then loaded a web page with

a paid search program, followed by a piece of JavaScript code, and clicked on the search result, triggering a payout to the Enterprise.

83. *Generating Click Traffic*. Finally, the BadBox 2.0 Enterprise uses infected devices to carry out click fraud. The BadBox 2.0 Enterprise uses its C2 Servers to deploy malware packages that instruct bots to navigate to their low-quality web domains and click on advertisements hosted on those domains. This, too, results in a payout to the Enterprise as publishers of the web domains.

84. One example of this activity is described below:

a. In a laboratory setting in the United States, researchers observed a device receive JavaScript instructions directing the device to visit a domain published by the Backdoor Malware Group and to identify an ad operated by the Enterprise. Once the device navigated to the domain, the C2 Server instructed the device to click on an ad. The device generated clicks on the ad and caused Google to pay the Enterprise.

85. Google has identified activity related to BadBox 2.0 on its own platforms, including by identifying incoming or outgoing malicious internet traffic, and has taken action to stop the impact of that activity. Specifically, Google has identified and terminated thousands of Google Ad Manager publisher accounts that the Enterprise created to receive payments in connection with ad requests generated by BadBox 2.0.

Harm to Google, its Users, and the Public

86. The BadBox 2.0 Scheme harms the owners of the devices that are infected with the malware, Google, and countless other persons and entities.

87. The owners of infected devices are harmed in numerous ways. Their devices and IP addresses are being deployed in the service of the BadBox 2.0 Enterprise's ad fraud schemes, including through the continued unauthorized access to and criminal misuse of their devices, and their personal information may be stolen in that process as well. Additionally, the malware deployed on users' devices wastes electricity and CPU processing power and occupies memory space on the device, which slows down users' devices.

88. The BadBox 2.0 Scheme causes substantial harm to Google as well.

89. The BadBox 2.0 Scheme causes financial loss to Google, including but not limited to the losses incurred in connection with Defendants' ad fraud. Google also has devoted (and continues to devote) substantial financial resources to investigate the BadBox 2.0 botnet and to identify measures necessary to remediate the harms caused by the botnet.

90. The BadBox 2.0 Scheme also causes reputational damage to Google.

91. Google's reputation is tarnished when fraud occurs on its platforms, leading to a loss of customer goodwill.

92. Although Google does not own AOSP, and those devices are not covered by Google Play Protect, Google retains a significant role in overseeing and approving development of AOSP to protect AOSP's and Google's reputation.

93. The BadBox 2.0 Scheme causes Google to expend substantial resources to detect, deter, and disrupt it due to the threat the BadBox 2.0 Scheme poses to the security of Google's platform. Because the BadBox 2.0 botnet continues to grow each day, Google must continuously expend resources to combat it.

94. Beyond Google, the continued proliferation of malware on AOSP devices harms the internet ecosystem as a whole.

95. If the BadBox 2.0 Scheme is not disrupted, it will continue to proliferate. The BadBox 2.0 Enterprise will continue to generate revenue, will use those proceeds to expand its reach, producing new devices and new malware to fuel its criminal activity, and Google will be forced to continue expending substantial financial resources to investigate and combat the Enterprise's fraudulent activity.

96. If BadBox 2.0 continues to operate unchecked, the threat it poses will grow as well. The BadBox 2.0 Scheme has already gained control of more than ten million devices, capable of supporting large-scale cyber-attacks. The BadBox 2.0 Enterprise could, for example, conduct or sell access to others to conduct large ransomware or DDoS attacks on legitimate businesses and other targets.

CLAIMS FOR RELIEF

COUNT I
Computer Fraud and Abuse Act Violations
18 U.S.C. § 1030(a)(4), (a)(5)(A)

97. Google incorporates the foregoing paragraphs (¶¶ 1–96) of the Complaint as if set forth in full.

98. Defendants have violated and continue to violate the CFAA, 18 U.S.C. § 1030(a)(4), (a)(5)(A), resulting in loss as defined in 18 U.S.C. § 1030(e)(11) to one or more persons during a one-year period amounting in the aggregate to at least $5,000 in value.

99. First, Defendants have violated and continue to violate 18 U.S.C. § 1030(a)(4) by knowingly and with intent to defraud accessing protected computers without authorization and/or

by exceeding authorized access, and by means of such conduct furthering the intended fraud and obtaining value.

100. In particular, the computers affected by Defendants' BadBox 2.0 Scheme are "protected computers" within the meaning of the CFAA because they are used in or affect interstate commerce or communication through the internet. *See* 18 U.S.C. § 1030(e)(2)(B).

101. Defendants have accessed such computers without authorization and/or exceeded authorized access by infecting such computers with malware that directs the device to connect to and communicate with a specific C2 Server without the consent of the device's owner or user.

102. Defendants' access to these computers is knowing and with intent to defraud. Defendants' BadBox 2.0 botnet is designed to further a variety of fraudulent schemes, including ad fraud and sale of access to proxy services that facilitate cybercrime.

103. Defendants' intent to defraud is evidenced by their surreptitious access to devices through pre-installed or downloaded malware without the consent of the devices' owners or users.

104. Defendants' access to the infected computers has furthered Defendants' various fraudulent schemes and has provided Defendants with value through those schemes, such as money from selling residential proxy services and money from ad fraud.

105. Defendants' violations of 18 U.S.C. § 1030(a)(4) have caused loss to Google aggregating at least $5,000 in value during a one-year period. *See* 18 U.S.C. § 1030(c)(4)(A)(i)(I); *id*. § 1030(g).

106. Specifically, Google has suffered loss in the form of reasonable costs of responding to Defendants' BadBox 2.0 Scheme, including conducting damage assessments. *See* 18 U.S.C. § 1030(e)(11). Over the period from May 1, 2024 to May 1, 2025, those losses have exceeded $5,000.00.

107. In addition, Defendants' violation of 18 U.S.C. § 1030(a)(4) has caused damage within the meaning of 18 U.S.C. § 1030(e)(8) affecting more than ten million protected computers. The enormous scope of Defendants' botnet drastically exceeds the threshold for even criminal liability. *See* 18 U.S.C. § 1030(c)(4)(A)(i)(VI).

108. Second, Defendants have violated and are continuing to violate 18 U.S.C. § 1030(a)(5)(A) by knowingly infecting protected computers with BadBox 2.0 backdoor malware, transmitting software designed to carry out their schemes, and transmitting commands to infected computers that direct them to communicate with C2 Servers, intentionally causing damage.

109. In particular, Defendants have intentionally caused malware and commands to be transmitted to infected devices.

110. The infected devices are "protected computers" within the meaning of the CFAA because they are used in or affect interstate commerce or communication through the internet. *See* 18 U.S.C. § 1030(e)(2)(B).

111. Defendants have also intentionally transmitted commands to protected computers through the internet, thereby enabling Defendants to use those computers in their fraudulent schemes.

112. Defendants' transmissions of malware and commands to infected devices have intentionally caused damage without authorization within the meaning of 18 U.S.C. § 1030(a)(5)(A).

113. Defendants' transmissions of malware and commands to infected devices have impaired those computers' cybersecurity detection tools, anti-virus software, and system monitoring programs. These impairments constitute damage. *See* 18 U.S.C. § 1030(e)(8).

114. Defendants' violations of 18 U.S.C. § 1030(a)(5)(A) have caused loss to Google aggregating at least $5,000 in value during a one-year period. *See* 18 U.S.C. § 1030(c)(4)(A)(i)(I); *id.* § 1030(g).

115. Specifically, Google has suffered loss in the form of reasonable costs of responding to Defendants' BadBox 2.0 Scheme, including conducting damage assessments. *See* 18 U.S.C. § 1030(e)(11). Over the period from May 1, 2024 to May 1, 2025, those losses have exceeded $5,000.00.

116. In addition, Defendants' violation of 18 U.S.C. § 1030(a)(4) has caused damage within the meaning of 18 U.S.C. § 1030(e)(8) affecting more than ten million protected computers. The enormous scope of Defendants' botnet drastically exceeds the threshold for even criminal liability. *See* 18 U.S.C. § 1030(c)(4)(A)(i)(VI).

117. Google seeks injunctive relief and compensatory damages in an amount to be proven at trial. *See* 18 U.S.C. § 1030(g).

118. As a direct result of Defendants' actions, Google has suffered and continues to suffer irreparable harm for which there is not an adequate remedy at law, and which will continue unless Defendants' actions are enjoined.

COUNT II
Violation of the Racketeer Influenced and Corrupt Organizations Act
18 U.S.C. § 1962(c)-(d)

119. Google incorporates by reference the foregoing paragraphs (¶¶ 1–118) of the Complaint as if set forth in full.

120. At all relevant times, Google is and has been a "person" within the meaning of 18 U.S.C. § 1961(3).

121. At all relevant times, Google is and has been a "person injured in his business or property by reason of a violation of" RICO within the meaning of 18 U.S.C. § 1964(c).

122. At all relevant times, each Defendant is a person within the meaning of 18 U.S.C. §§ 1961(3) and 1962(c).

123. Under 18 U.S.C. § 1964(c), Google is entitled to recover treble damages plus costs and attorney's fees from the Defendants.

The RICO Enterprise

124. The Defendants are a group of persons associated together in fact for the common purpose of carrying out an ongoing criminal enterprise, as described in the foregoing paragraphs of this Complaint. Specifically, Defendants created, control, and use the vast BadBox 2.0 botnet to execute numerous criminal schemes that harm and threaten to continue to harm Google, its users, and the public more broadly. These schemes include the sale of proxy services scheme (*supra* ¶¶ 52–58), the hidden ads scheme (*supra* ¶¶ 69–77), and the hidden web browser activity scheme (*supra* ¶¶ 78–820).

125. As described *supra* at paragraphs 41 through 45, Defendants, including the individuals and co-conspirators, have organized their operation into a cohesive group with specific and assigned responsibilities, operating in the United States and overseas, targeting and using victim devices in the United States. Over time, they have adapted their operations and schemes, enlisted new devices in their operation, and expanded the scope and nature of their activities.

126. Defendants act with the common purpose of profiting from their various fraudulent and criminal schemes that operate through the BadBox 2.0 network of infected devices. Specifically, Defendants have collaborated to establish, grow, and manage a botnet controlled through malware that Defendants have jointly developed. Members of the Enterprise all take part in directing the aspects of the scheme: some develop the botnet infrastructure; others sell proxy access to IP addresses to mask and facilitate nefarious internet activity; others render hidden ads

on apps and preinstalled on infected devices; still others launch hidden web browsers that navigate to gaming sites replete with pop-up ads; and others steer infected devices to domains managed by the Enterprise, all to enrich themselves.

127. Defendants constitute an association-in-fact enterprise within the meaning of 18 U.S.C. §§ 1961(4) and 1962(c) because they work together on an ongoing basis to execute the BadBox 2.0 Scheme. The Defendants play complementary roles in perpetuating the BadBox 2.0 Scheme, they have an established *modus operandi*, and they share the common purpose of developing, operating, and disseminating BadBox 2.0 for profit, as explained above. *Supra* ¶¶ 41–45.

128. All of the Defendants participate in the operation or management of the BadBox 2.0 Scheme, as evidenced by the threat actors' shared use, staging, and management of the infrastructure that underlies the BadBox 2.0 Scheme, including the shared C2 Server and botnet of infected devices.

129. The shared infrastructure underlying the BadBox 2.0 Scheme also evidences collaboration, overlap, and the sharing of resources between Defendants and other threat actor groups. Such collaboration and overlap is further evidenced by the fact that the different threat actor groups also shared targets when engaging in their various fraudulent schemes.

130. At all relevant times, each of the Defendants were and are associated-in-fact with the BadBox 2.0 Enterprise and participated in the operation or management of the Enterprise.

131. At all relevant times, the BadBox 2.0 Scheme was engaged in these activities, and its activities affected interstate and foreign commerce within the meaning of 18 U.S.C. § 1962(c).

Pattern of Racketeering Activity and RICO Predicate Acts

132. At all relevant times, Defendants conducted or participated, directly or indirectly, in the conduct, management, or operation of the BadBox 2.0 Scheme through a pattern of

racketeering activity within the meaning of 18 U.S.C. § 1961(5) and in violation of 18 U.S.C. § 1962(c), with such conduct and activities affecting interstate and foreign commerce.

133. Defendants have directly or indirectly engaged in an unlawful pattern of racketeering activity involving thousands of RICO predicate offenses, including violations of the CFAA(18 U.S.C. § 1030(a)(5)(A)), and wire fraud (18 U.S.C. § 1343). Each of these statutory violations are incorporated as RICO predicate acts under 18 U.S.C. § 1961(1). These activities have affected and continue to affect interstate or foreign commerce.

134. Google was injured in its business and property by reason of the Defendants' violations of 18 U.S.C. § 1962(c), as described herein, including through Defendants' ad fraud schemes and by devoting substantial financial resources to combat Defendants' criminal schemes. These injuries are a direct, proximate, and reasonably foreseeable result of these violations, and Google will continue to be harmed absent the relief requested here.

The Computer Fraud and Abuse Act Predicate Offenses (18 U.S.C. § 1030(a)(5)(A))

135. RICO provides, in 18 U.S.C. § 1961(1)(G), that any act indictable under 18 U.S.C. § 2332b(g)(5)(B) constitutes a RICO predicate act. Among the acts that are indictable under 18 U.S.C. § 2332b(g)(5)(B) are violations of 18 U.S.C. § 1030(a)(5)(A)—a provision of the CFAA—if such violation results in damage as defined in 18 U.S.C. § 1030(c)(4)(A)(i)(VI).

136. Defendants have violated and continue to violate the CFAA, 18 U.S.C. § 1030(a)(5)(A), resulting in damage as defined in 18 U.S.C. § 1030(c)(4)(A)(i)(VI), by infecting protected computers with malware, transmitting programs designed to carry out their schemes, and transmitting commands to infected computers. Each of these violations constitutes a separate RICO predicate offense.

137. *Transmission of Backdoor Malware Files.* Defendants have intentionally caused damage to "protected computers" by both pre-installing malware on devices that cause the infected

devices to download additional malware files or creating apps that, once downloaded, cause devices to download additional malware files and create a persistent connection between the device and a C2 Server, which results in the device becoming a "bot" that is commandeered into the BadBox 2.0 botnet, thereby impairing the integrity of their systems and information, and allowing Defendants to have persistent access those systems. The infected devices are "protected computers" within the meaning of the CFAA because they are used in or affect interstate commerce or communication through the internet. Through this conduct, Defendants have caused damage to ten or more protected computers in a one-year time period and have caused loss to one or more persons during a one-year time period amounting in the aggregate to at least $5,000 in value.

138. *Transmission of Malware Packages.* Defendants have transmitted malware packages to protected computers through the internet. Those packages damage the protected computers by launching hidden web browsers and hidden ads, as well as transmitting other packages to execute Defendants' criminal schemes. Through this conduct, Defendants have caused damage to ten or more protected computers in a one-year time period and have caused loss to one or more persons during a one-year time period, aggregating at least $5,000 in value.

139. *Transmission of Commands.* Defendants also have transmitted commands to protected computers through the internet, thereby causing damage to those computers and enabling Defendants to utilize these computers in its criminal schemes. Through this conduct, Defendants have caused damage to ten or more protected computers in a one-year time period and have caused loss to one or more persons during a one-year time period aggregating at least $5,000 in value.

140. Google has suffered injury to its business or property as a result of these predicate offenses, including due to Defendants' use of the botnet to sell residential proxy access and commit ad fraud.

Wire Fraud Predicate Offenses (18 U.S.C. § 1343)

141. Defendants, with intent to defraud and obtain money or property by means of false or fraudulent pretenses, commit wire fraud in violation of 18 U.S.C. § 1343 by transmitting or causing to be transmitted, by means of wire communication in interstate or foreign commerce, writings, signs, and signals for the purpose of executing fraudulent schemes. Defendants have violated and continue to violate the wire fraud statute in at least two ways, each instance of which constitutes a separate RICO predicate offense.

142. First, the Defendants commit wire fraud in violation of 18 U.S.C. § 1343 each time that they trick the owner of a device into unknowingly downloading and installing an app containing backdoor malware on the owner's device through misrepresentation and deception. For example, the BadBox 2.0 Scheme misleads victims by using the names of apps from official app marketplaces, such as Google Play, as described *supra* ¶ 49.

143. Second, to commit ad fraud, Defendants develop and publish apps and websites and then use bots to trigger bid requests on Google's ad platforms that deceive the platform into believing the advertisement will be shown to a real user. Each time that the Defendants facilitate a bid request due to bot activity on the Defendants' apps or websites, the Defendants as publishers of these apps or websites are compensated, as described *supra* ¶¶ 59–85. Therefore, Defendants generate these electronic bid requests for the purpose of obtaining money or property, including as described *supra* ¶¶ 59–85. Each time a request is generated, the Defendants commit an act of wire fraud in violation of 18 U.S.C. § 1343.

144. Google has suffered injury to its business or property as a result of each of these wire fraud predicate offenses, including the refunds it issues for bot traffic and the substantial sums of money it has invested to stop these acts.

Conspiracy to Violate RICO

145. Google incorporates the foregoing paragraphs (¶¶ 1–144) of the Complaint as if set forth in full.

146. Defendants have not undertaken the practices described herein in isolation, but rather as part of a common scheme. In violation of 18 U.S.C. § 1962(d), each Defendant unlawfully, knowingly, and willfully agreed and conspired together and with others to violate 18 U.S.C. § 1962(c) as described above, in violation of 18 U.S.C. § 1962(d).

147. Defendants knew that they were engaged in a conspiracy to commit multiple predicate offenses, and that the predicate offenses were part of a pattern of racketeering activity. Defendants' participation in the conspiracy and agreement to commit those offenses was necessary to facilitate this pattern of racketeering activity. This conduct constitutes a conspiracy to violate 18 U.S.C. § 1962(c), in violation of 18 U.S.C. § 1962(d).

148. Defendants agree to direct or participate in, directly or indirectly, the conduct, management, or operation of the BadBox 2.0 Scheme through a pattern of racketeering activity in violation of 18 U.S.C. § 1962(c). Each Defendant knew about and agreed to facilitate the BadBox 2.0 Scheme. The purpose of the conspiracy was to commit a pattern of racketeering activity in the conduct of the affairs of the BadBox 2.0 Scheme, including the acts of racketeering set forth above, including the sale of proxy services to commit crimes and the commission of multiple ad fraud schemes intended to enrich the Enterprise.

149. Google has been and continues to be directly injured by Defendants' conduct. But for the alleged pattern of racketeering activity, Google would not have incurred damages.

150. Google seeks injunctive relief and compensatory and punitive damages in an amount to be proven at trial.

151. As a direct result of Defendants' actions, Google has suffered and continues to suffer irreparable harm for which there is not an adequate remedy at law and which will continue unless Defendants' actions are enjoined.

PRAYER FOR RELIEF

WHEREFORE, Google prays for judgment as set forth below:

A. Judgment in favor of Google and against Defendants;

B. A declaration that Defendants have engaged in acts or practices that violate the CFAA and RICO;

C. A declaration that Defendants' conduct has been willful and that Defendants have acted with fraud, malice, and oppression;

D. A temporary restraining order and preliminary and permanent injunctions enjoining Defendants and their officers, directors, principals, agents, servants, employees, successors, and assigns, and all persons and entities in active concert or participation with them, from engaging in any of the activity complained of herein or from causing any of the injury complained of herein and from assisting, aiding, or abetting any other person or business entity in engaging in or performing any of the activity complained of herein or from causing any of the injury complained of herein;

E. Award of appropriate equitable relief available under applicable statutes and law, including injunctive relief;

F. Judgment awarding Google actual and/or statutory damages from Defendants adequate to compensate Google for Defendants' activity complained of herein and

for any injury complained of herein, including but not limited to interest and costs, in an amount to be proven at trial;

G. Judgment awarding enhanced, exemplary and special damages, in an amount to be proven at trial;

H. Judgment awarding attorneys' fees and costs; and

I. Order such other relief that the Court deems just and reasonable.

Dated: May 27, 2025

Respectfully submitted,

Laura Harris
KING & SPALDING LLP
1185 Avenue of the Americas, 34th Fl.
New York, NY 10036-2601
Tel: (212) 556-2100
Fax: (212) 556-2222
lharris@kslaw.com

Sumon Dantiki (*pro hac vice* to be submitted)
Christine M. Carletta
KING & SPALDING LLP
1700 Pennsylvania Ave., NW, Suite 900
Washington, DC 20006-4707
Tel: (202) 737-0500
Fax: (202) 626-3737
sdantiki@kslaw.com
ccarletta@kslaw.com

Counsel for Plaintiff Google LLC